PATENT
Attorney Docket No. P1895US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Arditi et al.

Application No. 10/659,796 Art Unit: 2136

Filed: September 11, 2003 Examiner: Fikremariam A. Yalew

For: ELECTRONIC SIGNATURE METHOD, PROGRAM AND SERVER FOR IMPLEMENTING THE METHOD

REQUEST FOR PRE-APPEAL BRIEF CONFERENCE

Mail Stop AF
Commissioner of Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Applicants respectfully request a pre-appeal brief conference for the reasons set forth below.

Applicants respectfully submit that clear errors exist in the Examiner's final rejection of claims 1-14 under 35 U.S.C. § 103(a) based on U.S. Patent No. 6,970,562 to Sandhu et al. in view of published U.S. Patent Application No. 2004/0103316 to Inada et al. As indicated in the Remarks on page 2, lines 9-14 of the Response filed on September 4, 2007 ("the Remarks"), Sandhu fails to teach or suggest formatting a calculated signature with the aid of the signature certificate received by the client station, and Sandhu also fails to teach or suggest at least the generation of a private/public key pair, calculation of an electronic signature and destruction of a cryptographic key as claimed. Furthermore, the teachings of Inada fail to make up for these deficiencies.

As further discussed on page 2, line 16 through page 3, line 4 of the Remarks, the embodiments of the present invention provide a system, method and software program for applying an electronic signature from a client station in a network. The client station is authenticated at a server of the network, and thus establishes an authenticated communication channel between itself and the server. The client then can generate a private key/public key pair, and send to the server, via the authenticated channel, a request for a signature certificate, generated by at least the public key. The client does not share the private key with the server. Upon receiving the request, the server sends a signature certificate to the client station, via the authenticated channel. The client station can then calculate a cryptographic signature based on the private key, and then destroys the private key. The client station then formats the calculated signature based on the signature certificate received from the server via the authenticated channel. These features are recited in independent claims 1, 8 and 12 of the present application in their current form.

As discussed on page 3, lines 7-24 of the Remarks, Sandhu teaches a system and method for crypto-key generation. Column 3, lines 22-33 of Sandhu, on which the Examiner relies, teach the creating of a certificate for *public key encryption* to validate *public keys*. This passage of Sandhu fails to teach or suggest the generation of a public/private key pair as explicitly recited in independent claims 1, 8 and 18. Furthermore, column 3, lines 35-49 of Sandhu teach the revocation of public key certificates are part of the duties of the Certificate Authorities. Nowhere does this passage teach or suggest calculating an electronic signature or destroying a cryptographic key as the Examiner contends. Also, column 3, lines 50-67 of Sandhu teach split private key cryptography, not the creation or use of public keys. Column 4, lines 1-9 teach authentication by challenge and response with a symmetric key, and column

4, lines 10-19 teach authentication by challenge and response with an asymmetric key. In addition, column 4, lines 20-33 teach SSL authentication using the signature of a message from the server side, and column 4, lines 33-42 teach SSL authentication using an authentication of the client by the server. Nowhere do these or any other passages of Sandhu teach or suggest destroying a cryptographic key after obtaining the signature as the Examiner contends.

Granted, column 8, lines 49-51 Sandhu may state that the private key is "destroyed completely." However, column 9, lines 20-25 of Sandhu explains how the same private key can be used on another processor, as it is regenerated based on a password as described in column 8, lines 63-67 of Sandhu. Therefore, the private key is not completely destroyed, but is only "destroyed" with respect to the first processor. However, in the embodiments of the present invention, the private key is completely destroyed, is not distributed and is not generated again from a seed, such as a password, or by any other means.

As further discussed on page 4, lines 1-15 of the Remarks, Applicants further submit that one skilled in the art would not use a challenge/response authentication technique with symmetric keys as taught by Sandhu with a challenge/response authentication technique with asymmetric keys as also taught by Sandhu. It is believed that the Examiner is making this contention in asserting that the symmetric key features discussed in column 4, lines 1-9 of Sandhu correspond to the features of step "B" in claim 1 of the present application, while also asserting that the asymmetric key features discussed in column 4, lines 10-19 of Sandhu correspond to steps "C" and "D" of claim 1 of the present application. Furthermore, even if an attempt to combine the techniques was made, the claimed embodiments of the present invention would not have been achieved. That is, column 1, lines 1-33 of Sandhu teach that a

client requests a signature certificate of a public key of the client. However, in SSL protocol, when the server signs a particular message to prove its identity (see column 4, lines 23-24 of Sandhu), the client uses the public key of the *server* to authenticate the signed message. Therefore, the client uses the chain of public key certificates to verify the public key of the *server*, that is, the certificate of the public key of the server as taught in column 4, lines 24-28 of Sandhu.

Concerning the Inada reference, as discussed on page 4, line 20 through page 5, line 2 of the Remarks, Inada teaches an electronic document format control apparatus and method, and its teachings fail to make up for the deficiencies in the teachings of Sandhu as discussed above. Specifically, the Examiner relies on Inada merely for its alleged teaching of formatting a calculated signature. Nevertheless, Inada fails to teach or suggest, for example, the features relating to the signature certificate of step C in independent claim 1 and the related features in independent claims 8 and 12, as well as the generation of a public/private key pair and the destruction of a cryptographic key as recited in independent claims 1, 8 and 12. Applicant also fails to see where Sandhu or Inada teach that the signature certificate has a validity period of at most one day as recited in dependent claims 6 and 13. Column 3, lines 50-67 of Sandhu, which are relied upon by the Examiner, seem to have no relationship to the validity period of a signature certificate.

For all the reasons given above and previously, Applicant respectfully submits that all claims should be allowable, and it is respectfully requested that this rejection be withdrawn and the application be allowed.

Respectfully submitted,

/brian c. rupp/

Brian C. Rupp, Reg. No. 35,665
DRINKER BIDDLE & REATH LLP
191 N. Wacker Drive, Suite 3700
Chicago, Illinois 60606-1698
(312) 569-1000 (telephone)
(312) 569-3000 (facsimile)
Customer No. 08968

Date: November 5, 2007

CH02/ 22502792.1